Instale y configure el OpenAM Identity Provider (IdP) para Cisco Identity Service (IdS) para habilitar el SSO

Contenido

Introducción

Este documento describe la configuración en OpenAM Identity Provider (IdP) para habilitar el inicio de sesión único (SSO).

Modelos de implementación de Cisco IdS

Producto	Implementación
UCCX	Copresidente
PCCE	Coresidente con CUIC (Cisco Unified Intelligence Center) y LD (Live Data)
UCCE	Coresidente con CUIC y LD para implementaciones 2k. Independiente para implementaciones de 4000 y 12 000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Express (UCCX) versión 11.6 o Cisco Unified Contact Center Enterprise versión 11.6 o Packaged Contact Center Enterprise (PCCE) versión 11.6, según corresponda.

Nota: Este documento hace referencia a la configuración con respecto a Cisco Identity Service (IdS) y el Identity Provider (IdP). El documento hace referencia a UCCX en las capturas de pantalla y los ejemplos; sin embargo, la configuración es similar con respecto al servicio de identificación de Cisco (UCCX/UCCE/PCCE) y al idP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Instalar

Nota: Este documento hace referencia a la versión 10.0.1 de OpenAM como parte de la calificación con SSO

Requisitos del sistema

Sistemas operativos	Entorno Java	Requisitos del contenedor de aplicaciones web	Navegadores admitidos	Requisitos del almacén de datos	Requisito mínimos d hardware
• Microsoft Windows Server 2003, 2008 R2 • Linux 2.6 y 3.0 • Oracle Solaris 10	La versión 10.0.1 de OpenAM requiere Java Development Kit 1.6, al menos 1.6.0_10. ForgeRock recomienda que utilice al menos la versión 1.6.0_27 debido a las correcciones de seguridad. ForgeRock ha probado esta versión de OpenAM principalmente con Oracle Java SE JDK. OpenAM Java SDK soporta Java Development Kit 1.5 o 1.6.	• Apache Tomcat 6.0.x, 7.0.x • GlassFish v2 • JBoss Enterprise Application Platform 4.x y 5.x • Servidor de aplicaciones JBoss 7.x • Embarcadero 7 • Oracle WebLogic Server 11g • Oracle WebLogic Server 12c Si se ejecuta como usuario no raíz, el contenedor de aplicaciones web debe poder escribir en su propio directorio principal, donde OpenAM almacena los archivos de configuración.	• Cromo y cromo 16 y posteriores • Firefox 3.6 y versiones posteriores • Internet Explorer (versión 7 y posteriores) • Safari 5 y posteriores	• OpenDJ de ForgeRock • Microsoft Active Directory • Servidor de directorio IBM Tivoli • OpenDS • Oracle Directory Server Enterprise Edition	• 1 GB RAM libre para OpenA Puede implementa OpenAM en cualquier hardware compatible con la combinació de software necesaria.

Instalar

Obtenga el software OpenAM

- Descargue las versiones de OpenAM 10.0.1 desde https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201
- Para cada versión de los servicios centrales de OpenAM, puede descargar el paquete completo como un archivo .zip, sólo el archivo .war de OpenAM, sólo las herramientas administrativas como un archivo .zip
- Después de descomprimir el archivo de todo el paquete, se obtiene un directorio opensso con un archivo README, un conjunto de archivos de licencia y los directorios

Requisitos previos

Asegúrese de que dispone del software necesario para los servicios principales de OpenAM antes de la instalación.

- Un entorno de tiempo de ejecución de Java 6
- Instalar Apache Tomcat como contenedor de aplicaciones web
- Los servicios de núcleo de OpenAM requieren un tamaño mínimo de pila de memoria virtual de Java (JVM) de 1 GB y un tamaño de generación permanente de 256 MB. Aplique las opciones de JVM cuando defina JAVA_OPTS en el archivo catalina antes del inicio del servidor de aplicaciones tomcat - -Xmx1024m -XX:MaxPermSize=256m

Por ejemplo, set JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m

- Instale Microsoft Active Directory como almacén de datos con pocos usuarios.

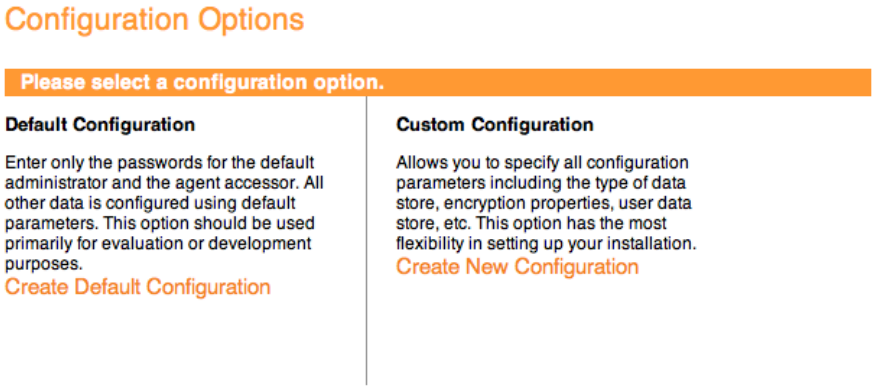
Instalación de la aplicación web OpenAM

El archivo deployable-war/opensso.war contiene todos los componentes y ejemplos del servidor OpenAM bajo el directorio opensso.

Implementación de OpenAM en el contenedor Tomcat

Copie el archivo opensso.war en el directorio donde se almacenan las aplicaciones web de tomcat. Cambie el nombre del archivo opensso.war por openam.war. Reinicie el servicio tomcat.

Verifique la pantalla de configuración inicial en su navegador en http://<FQHN>:8080/openam



Ejecutar el servicio OpenAM

Openam es una sencilla aplicación web alojada en un servidor tomcat. Por lo tanto, simplemente inicie su servidor tomcat y por lo tanto sea capaz de acceder al servicio web OpenAM.

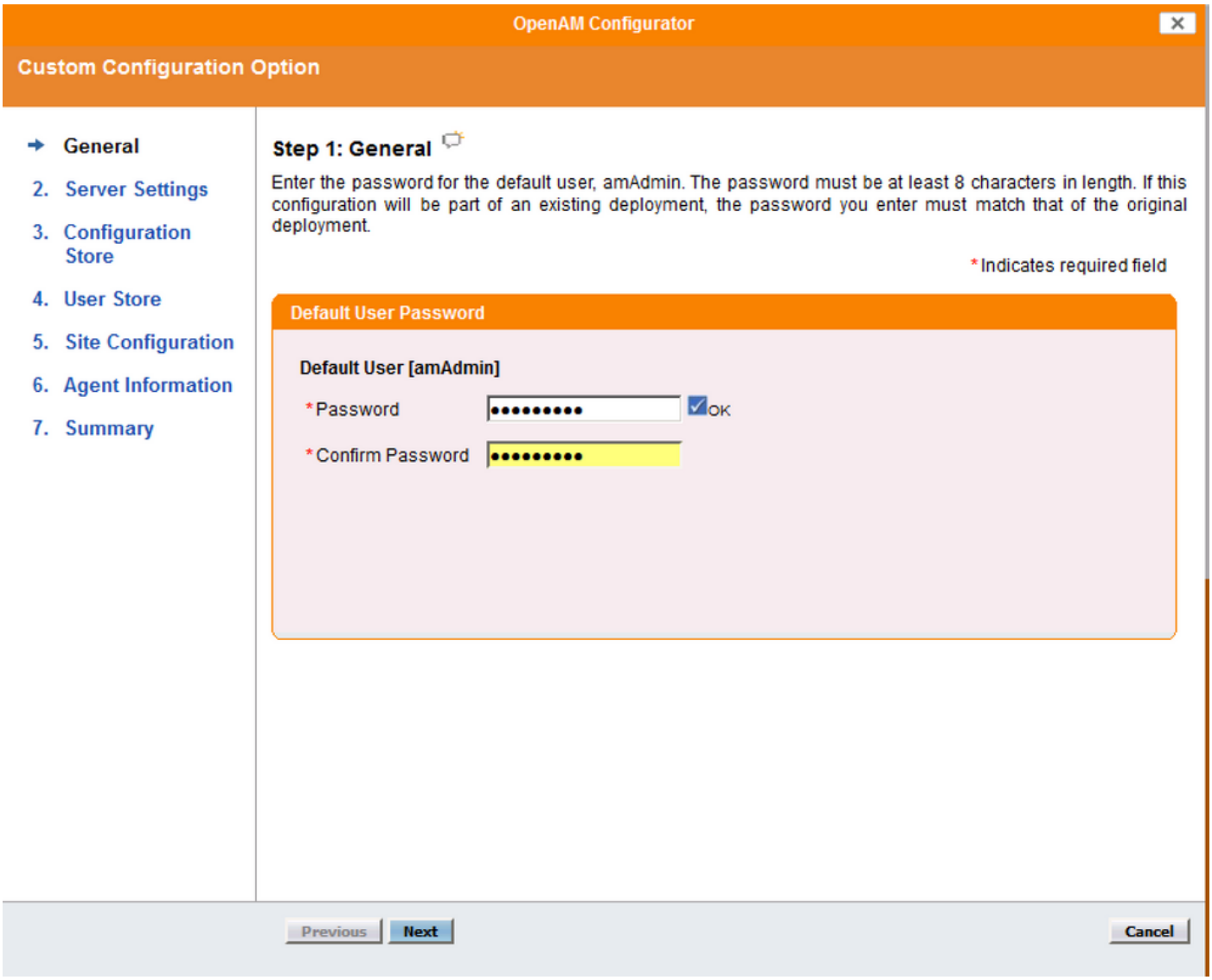
Configurar

Configurador OpenAM

El proceso de configuración personalizada de OpenAM permite establecer fácilmente muchas opciones de configuración comunes, por lo que con un mayor esfuerzo antes de la configuración, se guardan los pasos de configuración requeridos más adelante.

Configuración general

Haga clic en la opción Create New Configuration y elija la contraseña para la cuenta de administrador predeterminada (amAdmin). La contraseña debe tener al menos 8 caracteres.

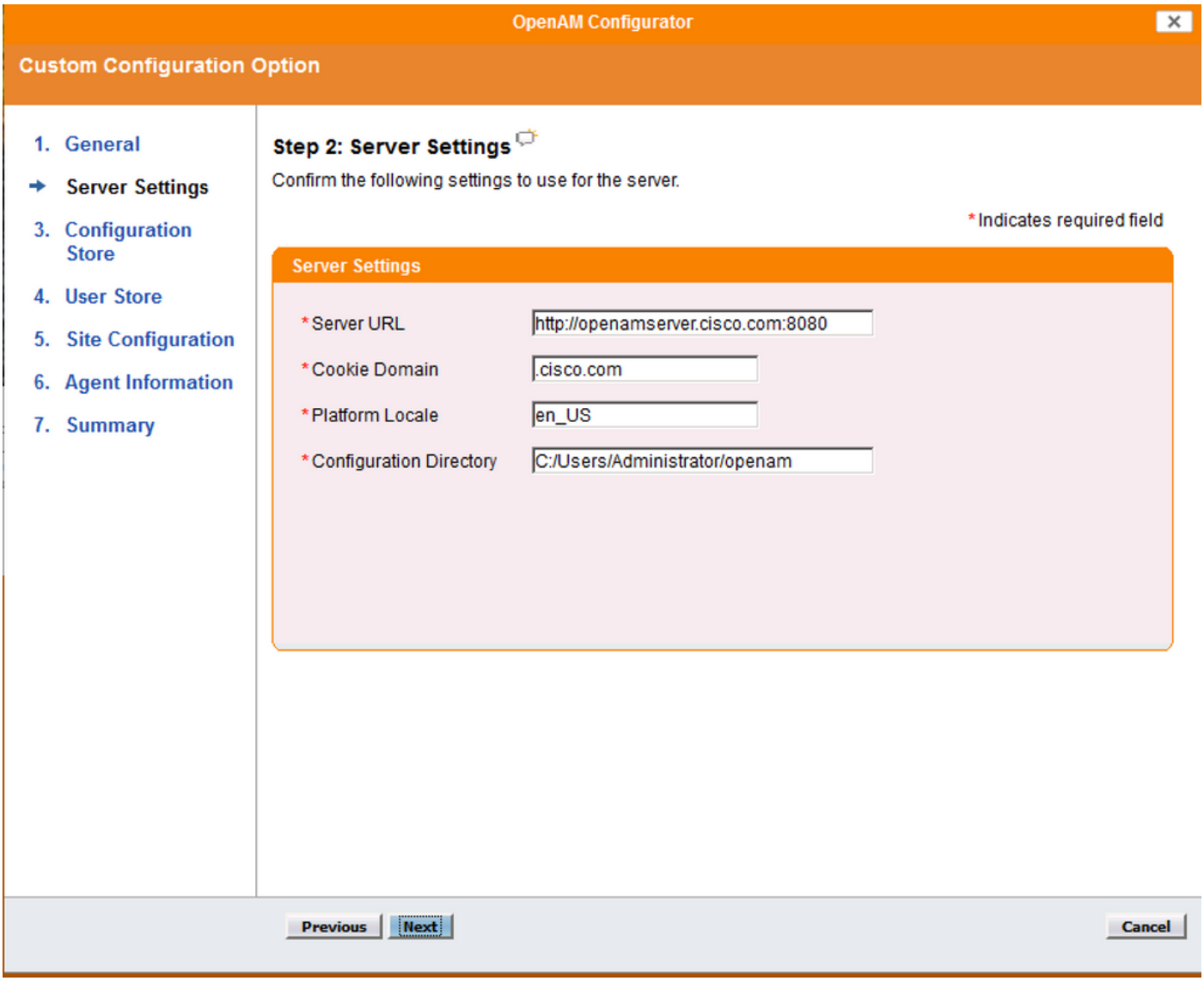


Una vez que se haya introducido una contraseña válida dos veces, aparecerá el botón next (siguiente) y la configuración podrá continuar.

Configuración del servidor

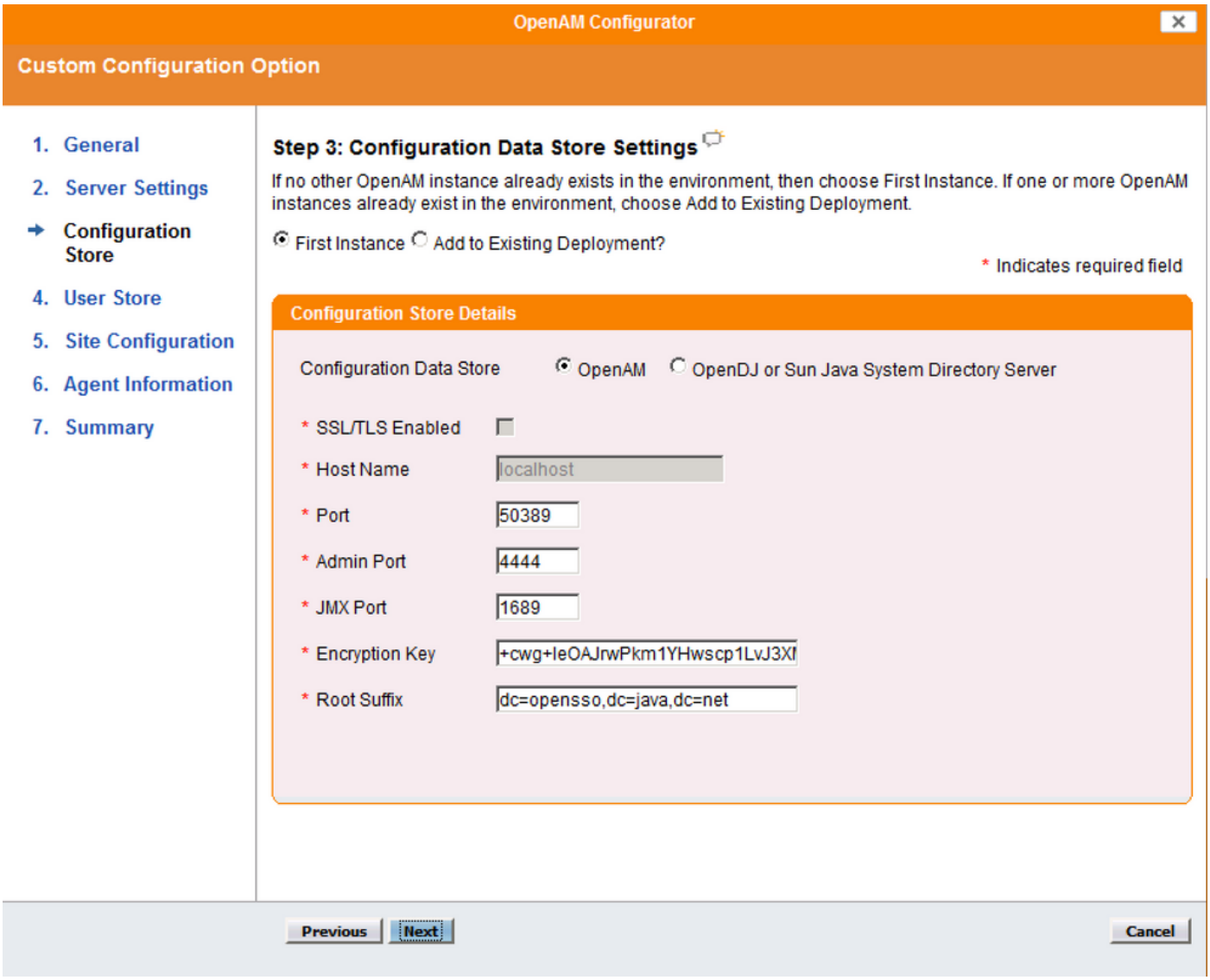
De forma predeterminada, la dirección URL del servidor es el nombre de dominio completo del servidor.

> Nota: Es importante que el usuario que ejecuta Apache Tomcat tenga acceso de escritura al directorio Configuration. Como resultado ~/openam/config es apropiado para este propósito. Las configuraciones regionales de plataforma compatibles son en_US (inglés), de (alemán), es (español), fr (francés), ja (japonés), zh_CN (chino simplificado) o zh_TW (chino tradicional).



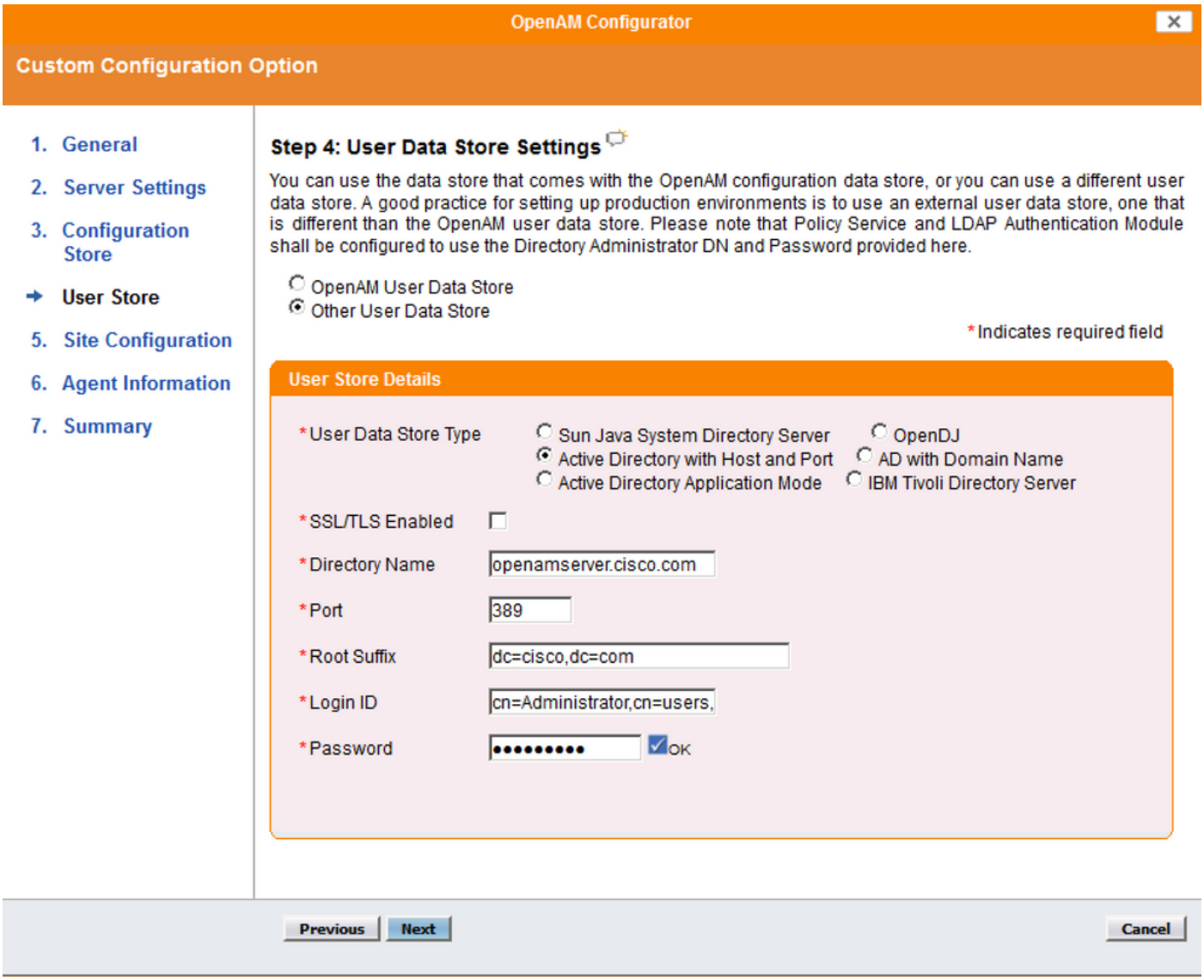
Configuración de almacén de datos

Para la configuración de un único servidor, no es necesario cambiar estos parámetros.



Configuración del almacén de datos de usuario

La configuración del almacén de datos de usuario conecta OpenAM al almacén de datos de Microsoft Active Directory.

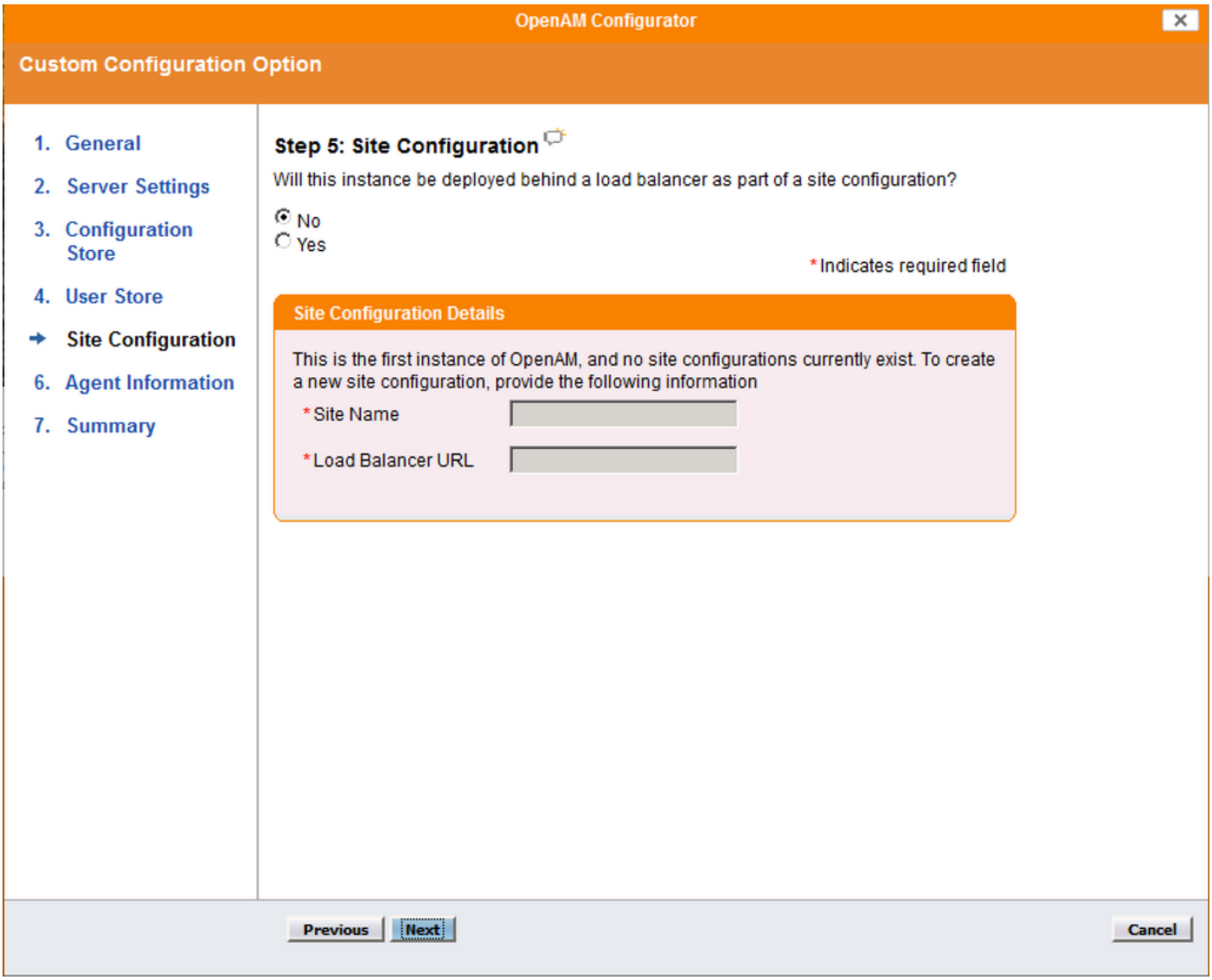


- Tipo de almacén de datos de usuario: Active Directory con host y puerto
- SSL/TLS habilitado: No aplicable
- Nombre del directorio: <Domain Name of AD Server>
- Puerto: 389
- Sufijo raíz: dc=cisco,dc=com
- ID de conexión: cn=<nombre de usuario de AD>,cn=users,dc=cisco,dc=com
- Contraseña <Contraseña de usuario de AD>

Nota: El configurador no proporciona una opción para continuar hasta que se hayan especificado correctamente todas las opciones y se haya conectado correctamente a la instancia de Active Directory.

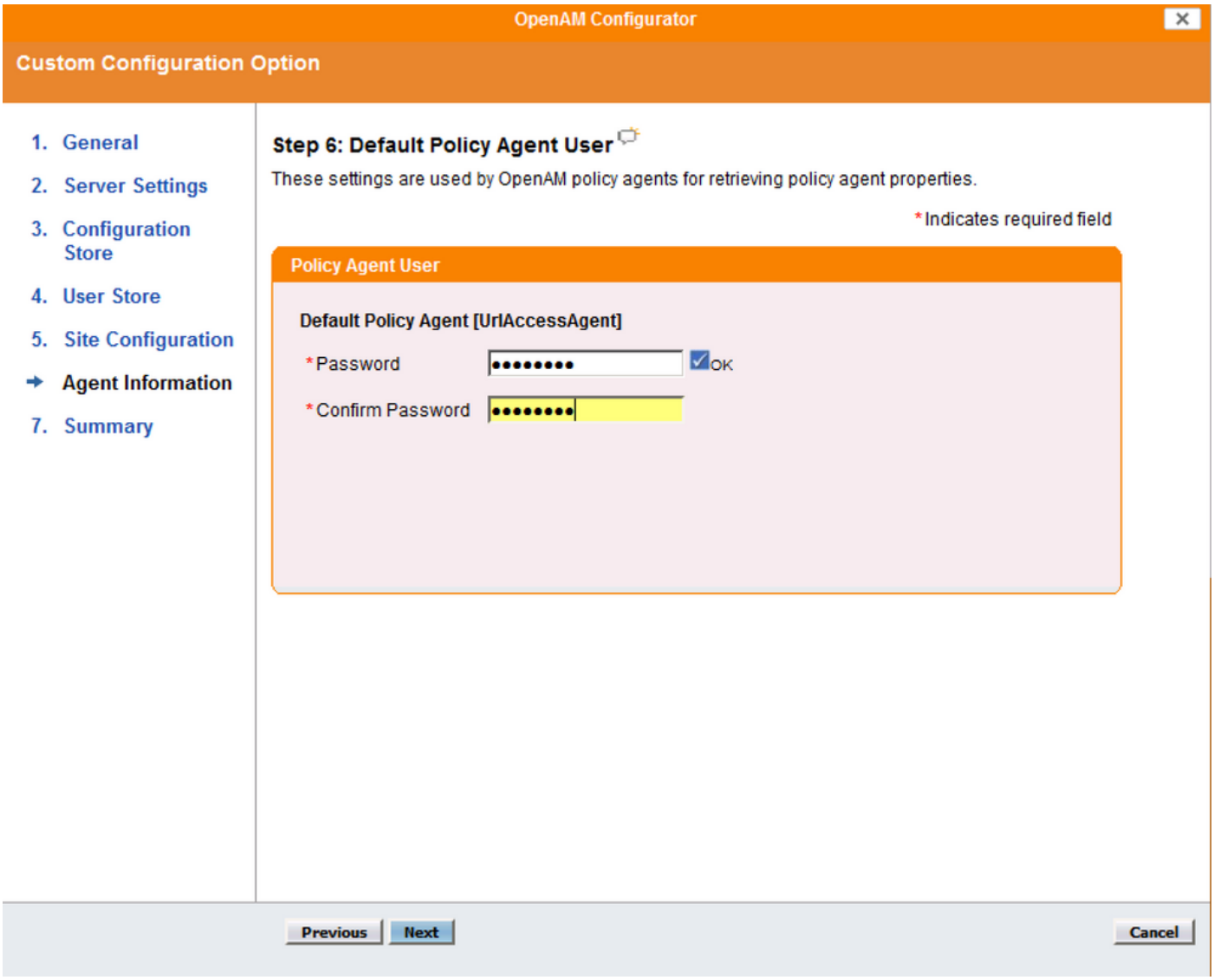
Configuración del sitio

En la pantalla Configuración del sitio, puede configurar OpenAM como parte de un sitio en el que la carga esté equilibrada entre varios servidores OpenAM. Para la primera instalación de OpenAM, acepte los valores predeterminados.



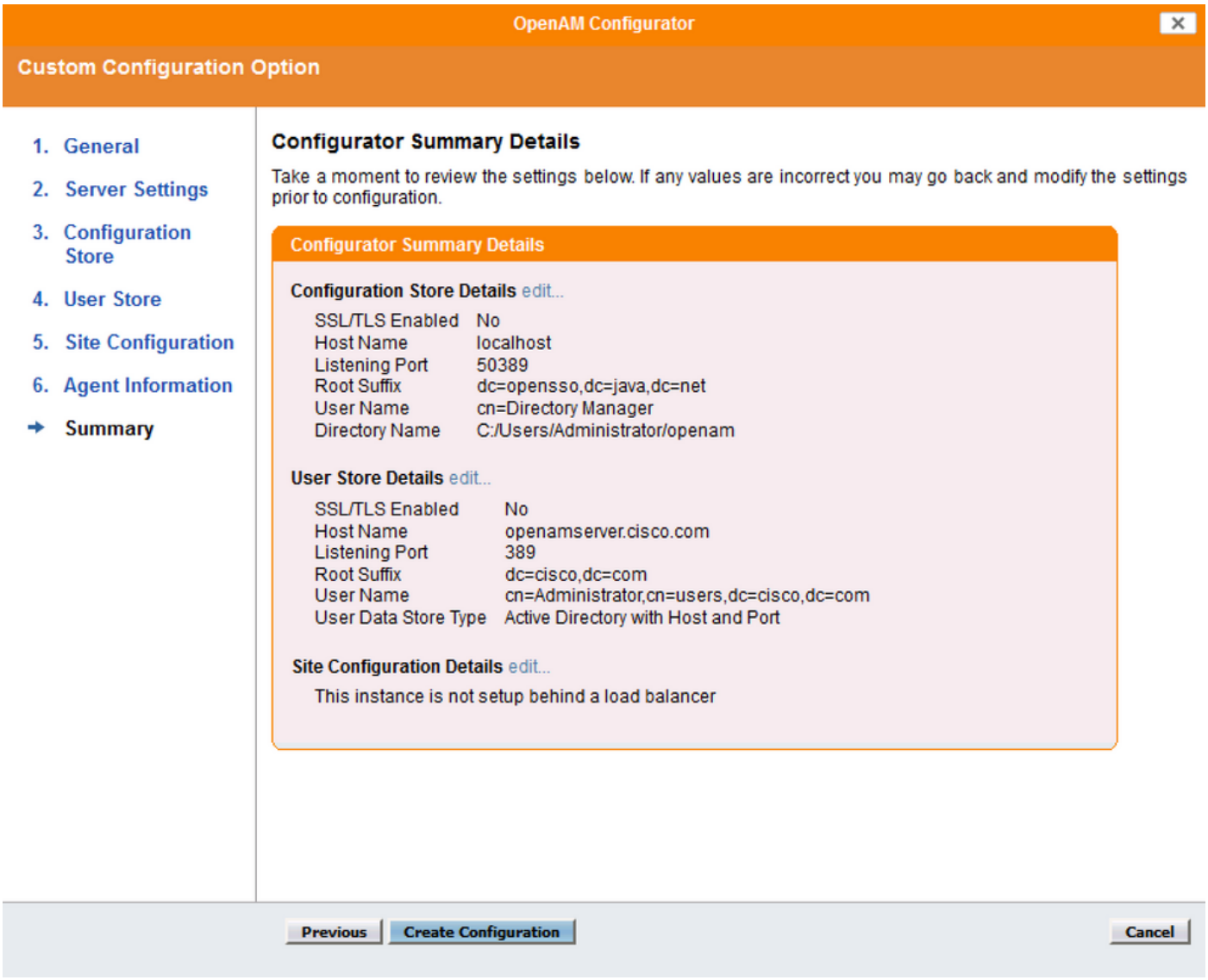
Información del agente

En la pantalla Agent Information (Información de agente), proporcione una contraseña de al menos 8 caracteres que los agentes de políticas utilizarán para conectarse a OpenAM.



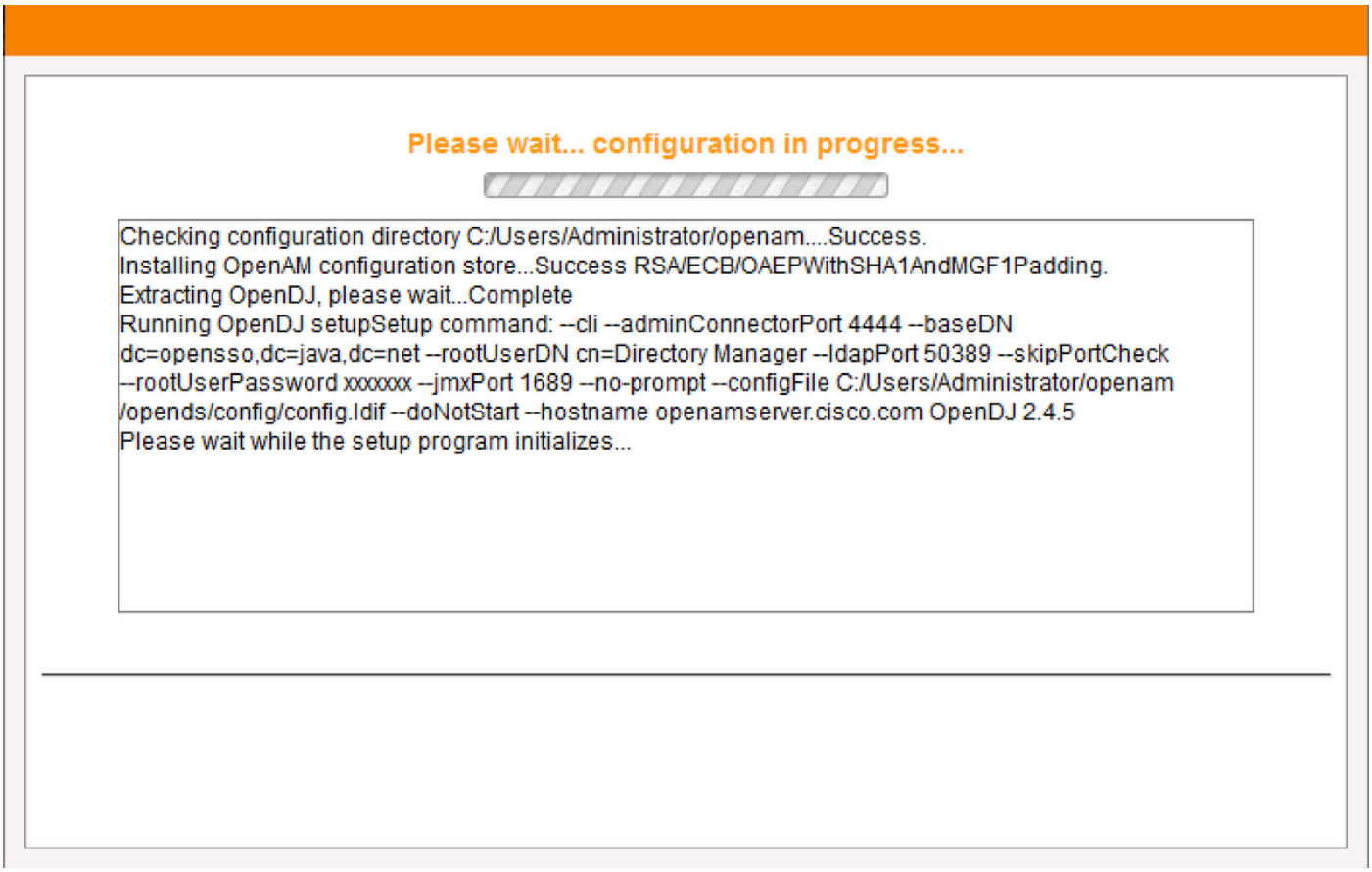
Summary

Revise la información y haga clic en Create Configuration .

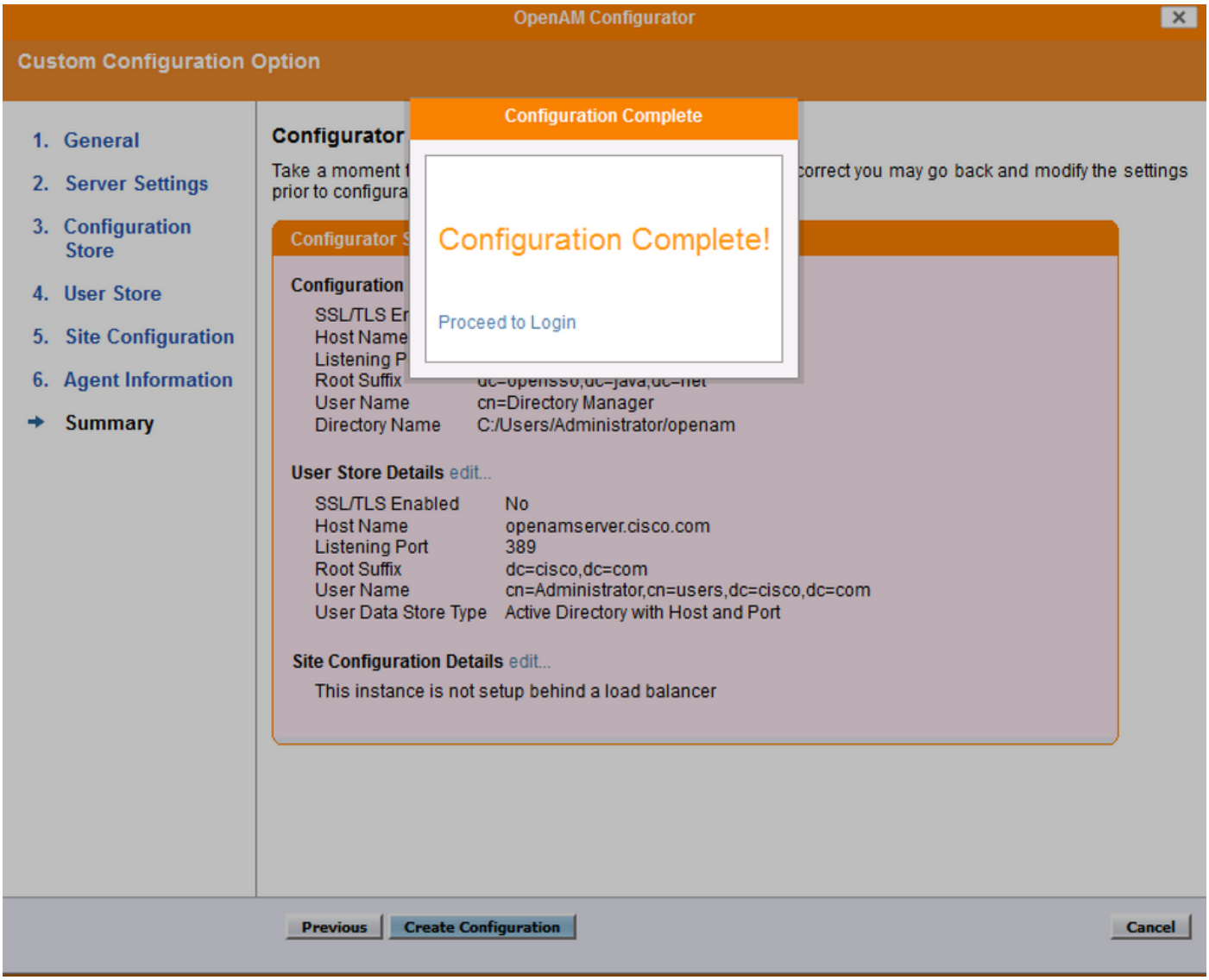


Progreso de configuración

La pantalla Progreso de la configuración muestra el progreso de la instalación. Todos los resultados de esta pantalla y los errores se escriben en el archivo: ~/openam/config/install.log.

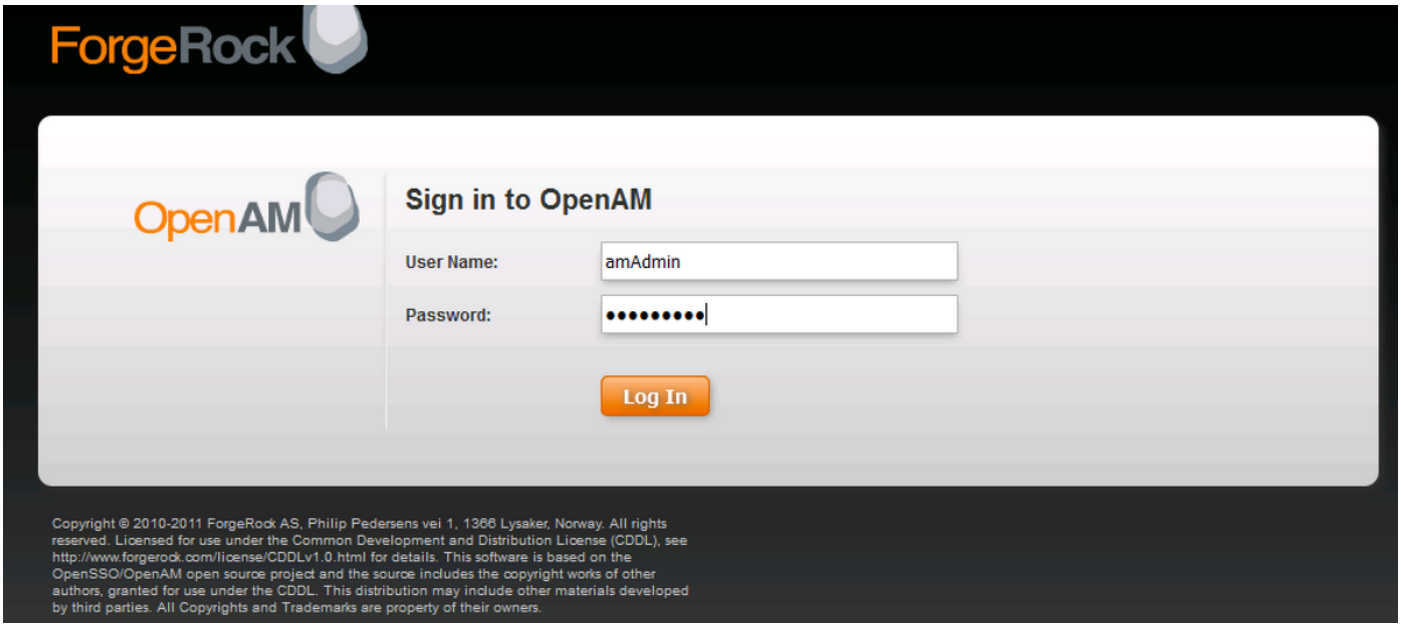


Configuración finalizada



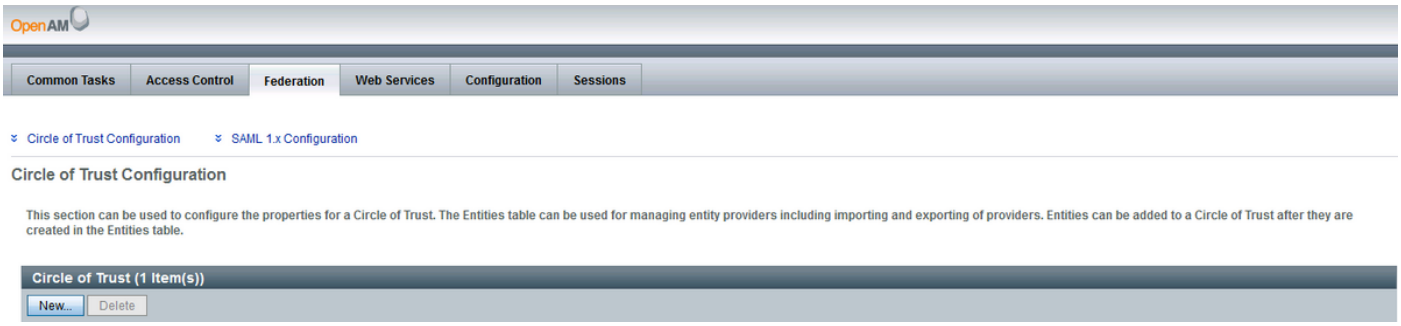
Configurar OpenAM como IdP

- Haga clic en Proceed to Login o Access through URL http://<FQDN of OpenAM>:8080/openam, y luego inicie sesión como administrador de OpenAM
- Cuando accede a OpenSSO Enterprise por primera vez, se le dirige al Configurador para realizar la configuración inicial de OpenSSO Enterprise
- Seleccionar configuración predeterminada
- Es necesario configurar las contraseñas para OpenAMserver
- Configure las contraseñas e inicie sesión en la interfaz del servidor OpemAM

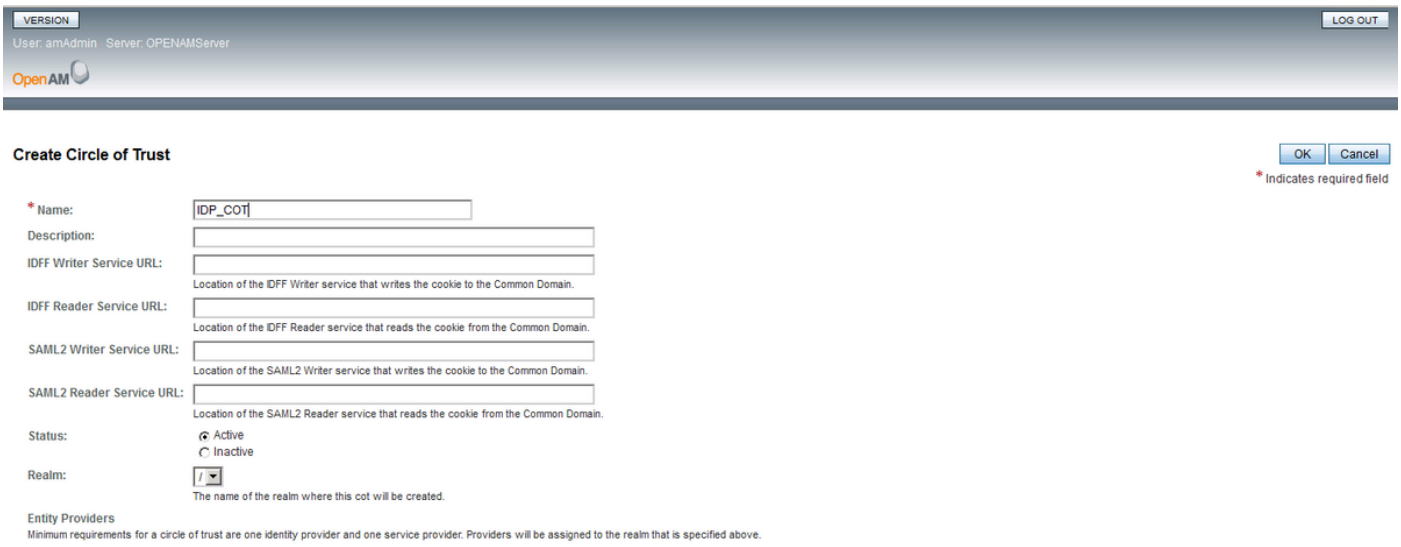


Configuración del círculo de confianza

Navegue hasta la pestaña de federación y haga clic en el botón Nuevo en la sección Círculo de confianza



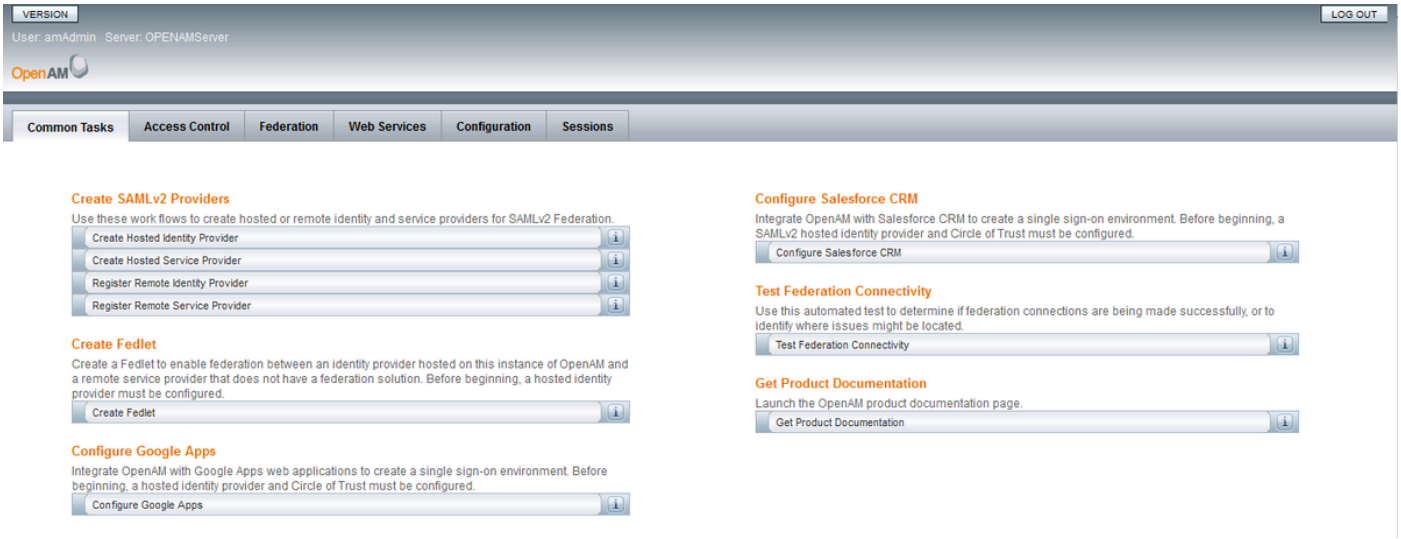
Cree un círculo de confianza con un nombre único para el círculo de confianza IdP y haga clic en Aceptar



Nota: El proveedor de servicios y el idP deben estar en el mismo círculo de confianza (CoT) para que funcione el SSO de SAML.

Crear proveedor de identidad alojado

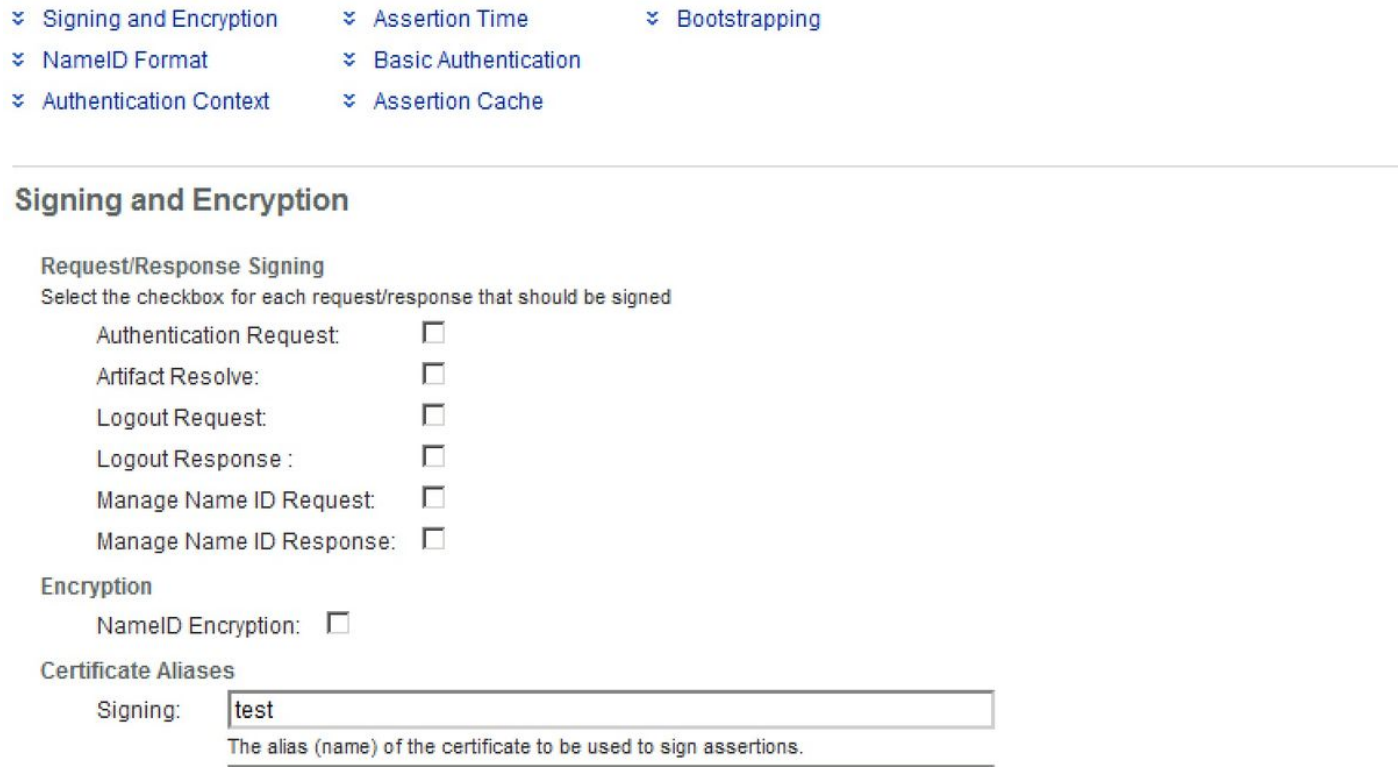
Vaya a la pestaña Tareas comunes y haga clic en Crear proveedor de identidad alojado y crear un IdP alojado (deje los valores predeterminados configurados y guarde los parámetros).



Se muestra el círculo de confianza creado anteriormente

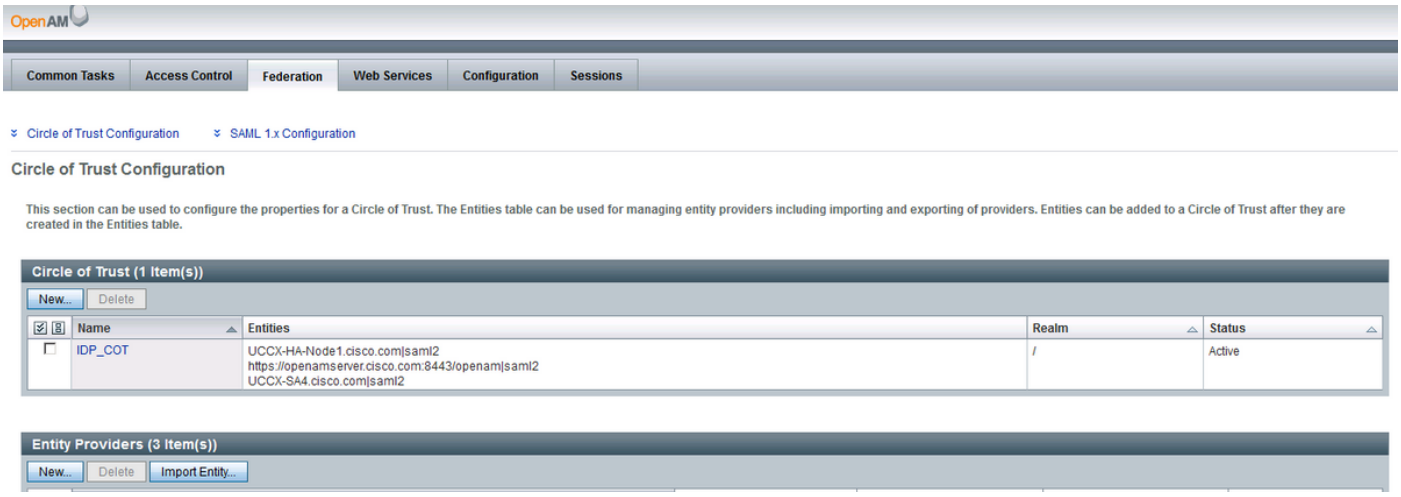
Configurar clave de firma

Navegue hasta la pestaña Federation y haga clic en el proveedor de identidad alojado agregado en la sección Proveedores de entidad. Navegue hasta la sección Contenido de la aserción y configure el valor del campo Firma como prueba en la sección Alias de certificado. Este es el certificado que se utilizaría para firmar la afirmación SAML.

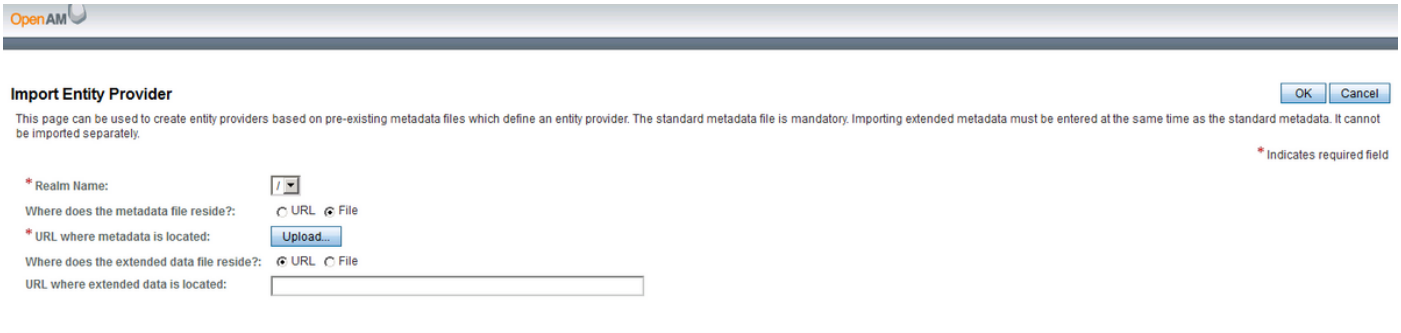


Importar entidad de proveedor de servicios

Navegue hasta la pestaña Federation y haga clic en el botón Import Entity... en la sección Entity Providers.

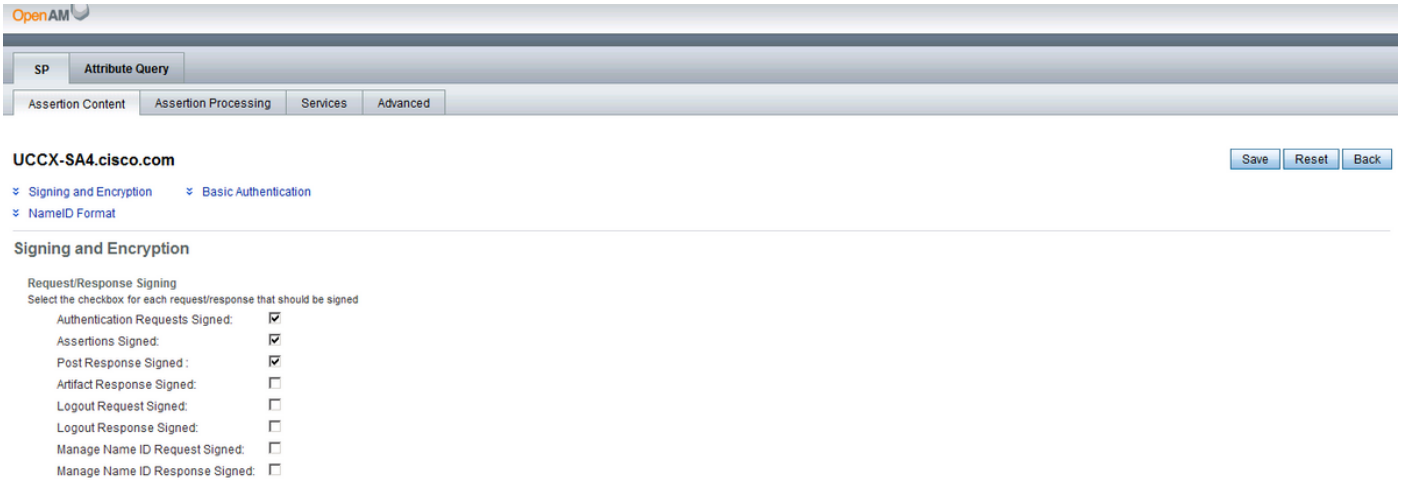


Cargue el archivo de entidad del proveedor de servicios (sp.xml) y guarde la página.



Firma de solicitud/respuesta

Haga clic en la entidad importada y active la firma para Solicitud/Respuesta



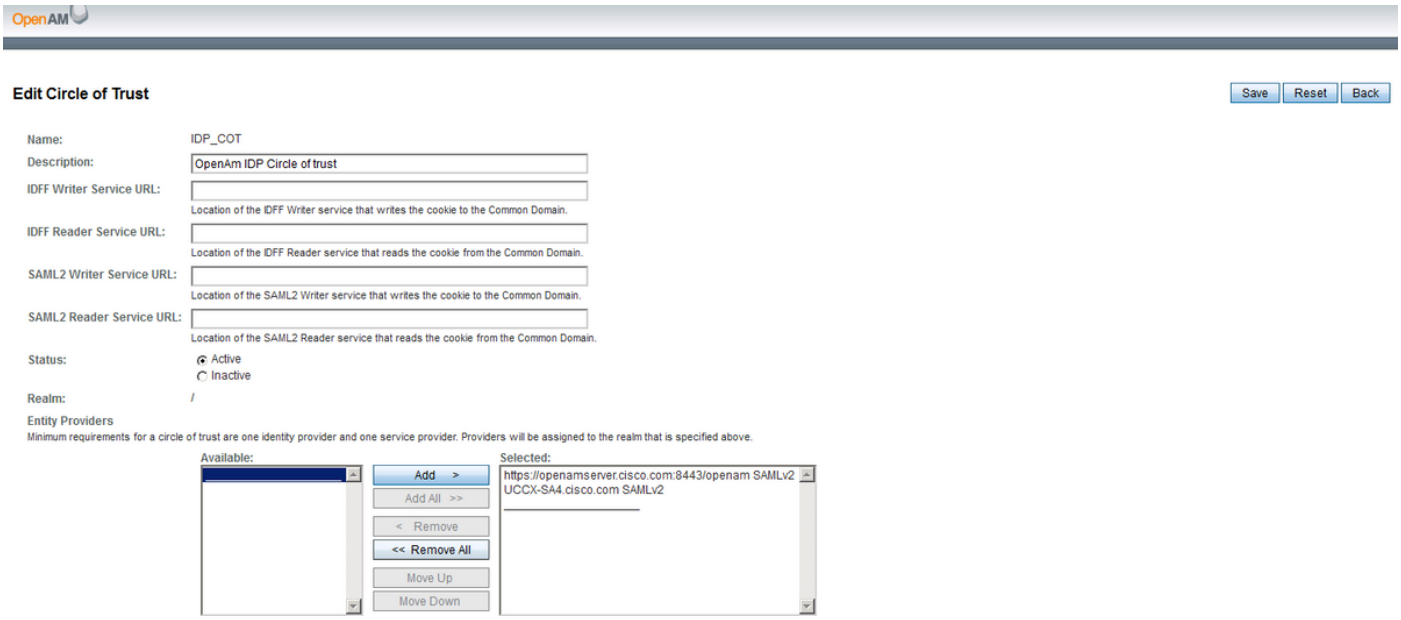
Asignación de atributos

Navegue hasta Procesamiento de aserción y agregue un atributo de asignación para uid y user_principal según la configuración de Directorio y OpenAM. Haga clic en Guardar.

Nota: Tanto los atributos uid como user_principal son obligatorios, ya que Service Provider (SP) identifica la identidad de un usuario autenticado con la ayuda de estos. Además, asegúrese de que los atributos sAMAccountName y userPrincipalName también estén asignados en el Editor de atributos de las propiedades de usuario de Active Directory.

Editar círculo de confianza

Desplácese hasta la ficha Federación y haga clic en Círculo de confianza agregado y asegúrese de mover el IdP (servidor OpenAm) y la entidad Proveedor de servicios de las secciones Disponible a Seleccionado en la sección Proveedores de entidades. Esto asigna al IdP y al Proveedor de Servicios que estén en el mismo Círculo de Confianza.



Descargar metadatos de OpenAM IdP

Puede descargar el archivo IdPmetadata del servidor OpenAM con la url [http://<FQDN de OpenAM>:8080/openam/saml2/jsp/exportmetadata.jsp?entityid=http://<FQDN de OpenAM>:8080/openam&realm=]

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
```

Ejemplo de XML de metadatos OpenAM

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://openamserver.cisco.com:8443/openam">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICcTCCAdqgAwIBAgIEWEe4zDANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTjESMBAGA1UE
                        CBMJa2FybmF0YWthMRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMx
                        DTALBgNVBAsTBGNjYnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wHhcNMTYxMjA3
                        MDcyMjUyWhcNMTgxMjA3MDcyMjUyWjB9MQswCQYDVQQGEwJJTjESMBAGA1UECBMJa2FybmF0YWth
                        MRIwEAYDVQQHEwliYW5nYWxvcmUxFjAUBgNVBAoTDWNpc2NvIHN5c3RlbXMxDTALBgNVBAsTBGNj
                        YnUxHzAdBgNVBAMTFm9wZW5hbXNlcnZlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
                        MIGJAoGBAKvhLKeu0mA1+V2YdfyuiFKQWXdM6EOc/1fmig94cGdNXxvW13KxzjUF2Vv4r364rTFi
                        73eIduF6e1/M481ECYed24LxKpgcSFMijaBdQl7AeQgyzPnWQCJODf85OguGVQhZUUt0RKKYP/d0
                        bgvarRrwXGIvoURJ+8Wy+zLV0T7nAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAM7MNSup7MOHYCLFl
                        i7hK89EMUIxmeywvAjEa8STH7Ba5d0Z1+R/bnXTS/9/pBETi5knuKd+Q59Pl9je2W7l36vFHoF1Q
                        jLlAGnPJOVEmOtimcGZGCj3m7ThlqnOlICyjnrXcLvQ10m75yfimFeeHdFPGbuzTsXjkIKjmhMF9
                        +cc=
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService index="0"
            isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/ArtifactResolver/metaAlias/idp1" />
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloRedirect/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPSloPOST/metaAlias/idp1" />
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPSloSoap/metaAlias/idp1" />
        <ManageNameIDService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniRedirect/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1"
            ResponseLocation="https://openamserver.cisco.com:8443/openam/IDPMniPOST/metaAlias/idp1" />
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/IDPMniSoap/metaAlias/idp1" />
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
        </NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
            Location="https://openamserver.cisco.com:8443/openam/SSORedirect/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://openamserver.cisco.com:8443/openam/SSOPOST/metaAlias/idp1" />
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/SSOSoap/metaAlias/idp1" />
        <NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/NIMSoap/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqSoap/IDPRole/metaAlias/idp1" />
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
            Location="https://openamserver.cisco.com:8443/openam/AIDReqUri/IDPRole/metaAlias/idp1" />
    </IDPSSODescriptor>
</EntityDescriptor>
```

Configuración adicional para SSO:

Este documento describe la configuración desde el aspecto IdP para que SSO se integre con Cisco Identity Service. Para obtener más información, consulte las guías de configuración de productos individuales:

- UCCX
- UCCE
- PCCE

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).